# *SOLUSI NETWORK SECURITY DARI ANCAMAN SQL INJECTION DAN DENIAL OF SERVICE (DOS)*

***Ir. Sumarno,M.M.[1] dan Sabto Bisosro[2]***

***1,2. Fakultas Teknik Universitas Muhammadiyah Sidoarjo***
***Email : thand_bond@yahoo.com***

## *ABSTRAK*

Spitzner, Lance (2003) *Honeypots* adalah suatu sistem keamanan jaringan komputer yang didesain untuk diserang/disusupi oleh *cracker*, dan bukan untuk menyediakan suatu suatu layanan produksi. Seharusnya hanya sedikit atau bahkan tidak ada sama sekali trafik jaringan yang berasal atau menuju *honeypots*. Oleh karena itu, semua trafik honeypots patut dicurigai sebagai aktivitas yang tidak sah atau tidak terautorisasi. Jika cukup informasi pada log file honeypots, maka aktivitas mereka dapat dimonitor dan diketahui pola serangannya tanpa menimbulkan resiko kepada production system asli atau data

Pada penelitian ini, dibangun suatu sistem honeypots yang menyerupai production system yang sesungguhnya. Layanan yang diemulasikan pada *honeypots* adalah web server. Mekanisme pengawasan/monitoring pada sistem honeypot ini dilakukan dengan menggunakan log. Digunakannya log ini adalah untuk memudahkan pemeriksaan kembali data (analisis forensik) yang diterima oleh sistem *honeypots.*

Implementasi dalam penelitian ini, sistem honeypot dirancang berdasar kepada high interaction *honeypo*t, yaitu sistem honeypot yang yang mengemulasikan service dengan alamat IP tersendiri. Rancangan *honeypot* dalam penelitian ini dipergunakan untuk memberikan service security terhadap layanan http (web server).

*Kata Kunci : Honeypots, cracker, log.*

## *ABSTRACT*

*Spitzner, Lance (2003) honeypots is a computer network security system designed for attack / compromised by a cracker, and not to provide an a production service. Should have little or even nothing at all network traffic originating in or towards honeypots. Therefore, all traffic honeypots suspect unauthorized activity or not terautorisasi. If enough information in the log files honeypots, then their activity can be monitored and known patterns of attacks without causing any risk to production systems or the original data In this study, constructed a system of honeypots that resembles the actual production system. The service is emulated on a web server honeypots. The mechanism of supervision / monitoring the honeypot system is done by using the log. These logs are used to facilitate re-examination of data (forensic analysis) received by the honeypots.*

*Implementation of this research, honeypot system is designed based on high-interaction honeypot, which is a honeypot system that emulates the service with its own IP address. The design of the research honeypot is used to provide security services to the http service (web server).*

*Keywords:  Honeypots, cracker, log.*

## *1. PENDAHULUAN*

Banyak aspek yang bisa mengancam keamanan sistem jaringan komputer, yaitu ancaman yang bersifat *interruption* dimana informasi dan data dalam system dirusak dan dihapus sehingga jika dibutuhkkan data atau informasi tersebut telah rusak atau hilang. Kemudian ancaman yang bersifat *interception* yaitu informasi yang ada disadap oleh orang yang tidak berhak mengakses informasi yang terdapat pada sistem ini. Selanjutnya *modifikasi* yaitu ncaman terhadap integritas dari sistem informasi tersebut. Dan yang terakhir adalah *fabrication* yaitu orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari yang dikehendaki oleh penerima informasi tersebut. dengan sistem ini diharapkan dapat mengetahui akan sistem keamanan jaringan komputer, khususnya mendeteksi segala sesuatu yang akan mengancam web server. Dalam penelitian ini diberikan gambaran bagaimana melakukan pencegahan atas serangan yang akan dilakukan oleh hacker dengan menekankan pada pendeteksian atas serangan yang dilakukan hacker sehingga admin dapat mempelajari serangan tersebut dan mencari solusi untuk mencegahannya.

Karena itu peneliti untuk melakukan observasi, dan melakukan pengumpulan data yang berkaitan dengan pendeteksian terhadap serangan *sql injection* dan *denial of service* . Dan dari beberapa ditemui, terdapat salah satu metode yaitu Honeypot yang melakukan pendeteksian dengan menipu hacker yang akan merusak sistem dengan suatu jaringan palsu, sehingga admin dengan mudah mempelajari trik yang dilakukan hacker tersebut.

Berdasarkanlatarbelakang di atas maka bagaimana cara merancang sistem honeypots guna mengamankan sebuah sistem informasi dari serangan *sql injection* dan *denial of service.* Dalam penulisan penelitian ini, dibatasi masalah pada penerapan aplikasi honeypots dengan simulasi pada sebuah jaringan guna mengenali dan memberikan pengamanan sistem informasi dari dua jenis serangan yaitu *sql injection* dan *denial of service. dengan tujuan* mengamankan sistem informasi dari serangan *sql injection* dan *denial of service*

## *2. TINJAUAN PUSTAKA*

Dony Ariyus (2005) dengan judul "Membangun Intrusion Detection System pada Windows 2003 Server" pengamanan jaringan computer dengan IDS (Intrusion Detection System) demikian pula hal yang sama pernah dilakukan oleh Didi, (2008) dengan judul "pengamanan Jaringan computer dengan Firewall" beda dengan penelitian saat ini yaitu penekanan pada penerapan aplikasi honeypots dengan simulasi pada sebuah jaringan guna mengenali dan memberikan pengamanan sistem informasi dari dua jenis serangan yaitu *sql injection* dan *denial of service. dengan tujuan* mengamankan sistem informasi dari serangan *sql injection* dan *denial of service*

## *3. LANDASAN TEORI*

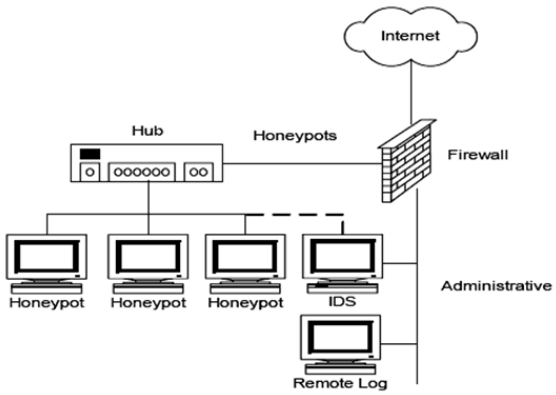
### *3.1. Definisi System Honeypots*

Spitzner, Lance (2003*) Honeypot* merupakan salah satu jenis teknologi terbaru di bidang keamanan sistem dan jaringan komputer yang digunakan sebagai pelengkap teknologi keamanan sebelumnya. Teknologi keamanan sebelumnya seperti firewall dan IDS *(Intrusion Detection System)* merupakan teknologi konvensional dimana sistem pertahanan di bangun untuk mencegah penyerang menembus masuk ke dalam area yang di lindungi.

*Honeypot* berbeda dari teknologi pertahanan konvensional sebelumnya dimana sistem pertahanan akan bernilai apabila penyerang telah masuk ke dalam sistem. Sistem honeypot akan melakukan monitoring terhadap aktivitas penyerang dengan menggunakan berbagai macam teknologi sehingga penyerang merasa aktivitas yang dilakukannya telah berhasil dan mengira sedang melakukan interaksi dengan sistem yang sebenarnya.

Honeynet mengimplementasikan Data Control dan Data Capture secara sederhana namun efektif. *Honeynet* yang menjadi gateway adalah firewall layer 3 (tiga). Firewall digunakan untuk memisahkan sistem *Honeynet* menjadi tiga jaringan yaitu Internet, *Honeypots* dan *Administrative.*

Setiap paket yang menuju ataupun meninggalkan sistem Honeynet harus melewati firewall. Firewall tersebut yang juga berfungsi sebagai Data Control akan diset untuk mengatur koneksi inbound dan outbound. Dikarenakan firewall tersebut merupakan bagian dari sistem Honeynet, maka konfigurasi firewall tersebut sedikit berbeda dengan konfigurasi firewall pada umumnya yaitu mengizinkan setiap koneksi inbound untuk masuk dan mengontrol / membatasi setiap koneksi outbound yang keluar dari sistem.



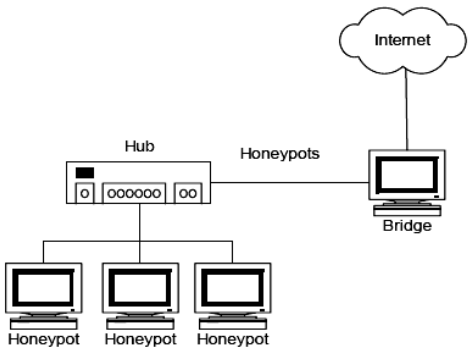

***Gambar 1. Implementasi honeypots 3 layer***

Data Capture yang diterapkan pada Honeynet terdiri dari beberapa layer / bagian. Layer pertama adalah log yang terdapat pada firewall itu sendiri. Firewall log akan mencatat setiap koneksi yang menuju atau meninggalkan Honeynet. Layer kedua adalah sistem IDS. Fungsi IDS adalah untuk menangkap setiap aktivitas yang terjadi pada jaringan dan juga karena pada umumnya IDS mempunyai signature database maka IDS dapat memberikan informasi yang lengkap dari suatu koneksi yang terjadi.

Layer ketiga adalah pada honeypot – honeypot itu sendiri. Ini dilakukan dengan cara mengaktifkan system log pada honeypot – honeypot yang digunakan. System log kemudian diset agar tidak hanya melakukan pencatatan secara lokal, tetapi juga secara remote ke sebuah remote log server.

Remote log server ini harus didisain lebih aman daripada *honeypot – honeypot* yang ada agar data – data yang didapat tidak hilang. Untuk membuat suatu solusi yang lebih mudah untuk diterapkan tetapi lebih susah untuk dideteksi oleh penyerang. Pada GenII *Honeynet* semua kebutuhan Honeynet (Data Control dan Capture) diterapkan hanya pada satu sistem saja (gateway) dan yang menjadi gateway adalah bridge layer 2 (dua).

Keuntungan menggunakan gateway berupa bridge layer 2 (dua) adalah layer 2 bridge tidak mempunyai IP stack sehingga ketika paket melewatinya tidak terjadi routing ataupun pengurangan TTL yang mengakibatkan gateway akan semakin sulit untuk dideteksi.




***Gambar 2. Implementasi honeypots 2 layer***

Spitzner (*www.tracking-attacker.com*) honeypot merupakan sebuah sistem atau komputer yang sengaja "dikorbankan" untuk menjadi target serangan dari attacker. Komputer tersebut melayani setiap serangan yang dilakukan oleh attacker dalam melakukan penetrasi terhadap server tersebut.

Metode ini ditujukan agar administrator dari server yang akan diserang dapat mengetahui trik penetrasi yang dilakukan oleh attacker serta agar dapat melakukan antisipasi dalam melindungi server yang sesungguhnya. Setiap tindakan yang dilakukan oleh penyusup yang mencoba melakukan koneksi ke honeypot tersebut, maka honeypot akan mendeteksi dan mencatatnya.

Peran dari honeypot bukanlah menyelesaikan suatu masalah yang akan dihadapi server, akan tetapi memiliki kontribusi dalam hal keseluruhan keamanan. Dan besarnya kontribusi tersebut tergantung dari bagaimana kita menggunakannya. Intinya, walaupun tidak secara langsung melakukan pencegahan terhadap serangan (firewall) tetapi dapat mengurangi dari intensitas serangan yang akan dilakukan oleh penyusup ke server yang sesungguhnya.

### *3.2. Nilai Kegunaan Honeypots*

Adapun penggunaan dari honeypot untuk beberapa kelompok / organisasi yaitu :

***Table 1. Kegunaan Honeypots dalam organisasi***

| Organisasi | Kegunaan |
|---|---|
| Perusahaan | pencegahan penyusupan |
| Militer | menerapkannya dalam perang cyberwarfare |
| Universitas | Melakukan riset |
| Lembaga penelitian | Melakukan riset |
| Dinas inteligen | Melakukan counter intelijen |
| Penegak hukum | Memperoleh aktivitas kriminal |

### *3.3. Klassifikasi Honeypots*

Honeypot dapat menjalankan bermacam service dalam pengamanan jaringan komputer dan dapat berjalan pada bermacam system operasi, honeypot dibedakan menjadi 2 (dua) yaitu Low-Interaction dan High-Interaction.

***Table 2. Klasifikasi Honeypots***

| **Low-interaction**<br>Mengemulasi system operasi dan service | **High-interaction**<br>Sistem operasi dan service sungguhan tanpa emulasi |
|---|---|
| 1. Mudah diinstall dan deploy, konfigurasi biasanya sederhana<br>2. Resiko minimal, emulasi mengontrol apa yang bisa dilakukan penyusup<br>3. Menangkap jumlah informasi terbatas | 1. Menangkap informasi lebih banyak<br>2. Bisa cukup kompleks<br>3. Resiko tinggi, penyusup bisa berinteraksi dengan system operasi sungguhan |

Honeypot juga dapat dibedakan menjadi (2) dua yaitu *Physical* yaitu Mesin sungguhan dalam jaringan dengan alamat IP sendiri. Dan *Virtual* yaitu honeypots yang disimulasikan oleh mesin lain yang berespon pada traffic jaringan yang dikirim ke virtual honeypot.

Suatu honeypots merupakan sumber system informasi yang menghasilkan nilai palsu pada saat terjadi penggunaan sumber daya yang tidak sah atau tidak diijinkan.

### *3.4. Firewall*

Sistem/mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN).

Firewall secara umum di peruntukkan untuk melayani :

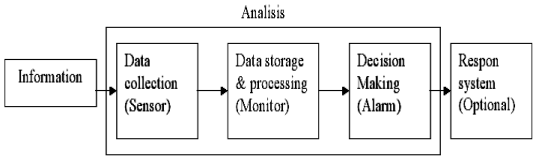
i. Mesin/komputer
   Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
ii. Jaringan
   Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

### *3.5. Intrusion Detection System*

Intrusion detection system adalah suatu perangkat lunak (software) atau suatu sistem perangkat keras (hardware) yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS memiliki 3 (tiga) komponen fungsi fundamental yang merupakan proses utama dalam IDS. Komponen fungsi itu antara lain :

i. Pengambilan Data (Information Sources). Komponen ini merupakan fungsi untuk melakukan pengambilan data dari berbagai sumber yang ada pada sistem yang diamati.
ii. Analisis. Bagian ini melakukan organisasi terhadap data yang diperoleh, mengambil kesimpulan terhadap pelanggaran / intrusion baik yang sedang terjadi maupun yang telah terjadi.

Respon. Komponen ini melakukan beberapa aksi pada sistem setelah pelanggaran yang terjadi telah terdeteksi. Respon ini dapat dikelompokkan menjadi 2 (dua), yaitu respon aktif dan respon pasif. Respon aktif dalam hal ini berarti melakukan beberapa aksi secara otomatis untuk mengintervensi sistem yang ada, sedangkan pasif adalah memberikan report pada administrator yang akan melakukan respon terhadap sistem.




***Gambar 3. Blok diagram Intrusion Detection System***

### *3.6. IPS (Intrusion Prevention System)*

Teknologi *Intrusion Detection System (IDS)* diperkirakan kadaluarsa dalam waktu dekat karena digantikan Intrusion Prevention System yang memiliki kemampuan lebih lengkap. IDS hanya mampu mendeteksi adaanya penyusupan dalam jaringan, lalu mengaktifkan peringatan kepada pengguna untuk segera mengambil langkah-langkah mitigasi sementara IPS langsung mengatasi penyusupan tersebut.

Awalnya IDS adalah pengembangan dari firewall, yakni sistem yang memisahkan antara jaringan internal dan eksternal. Firewall dinilai tidak cukup karena hanya sebagai pemisah saja, tidak memeriksa paket - paket data yang berbahaya sehingga bisa lolos. "Pada perkembangannya kemudian IDS tidak berguna karena pada saat alarm berbunyi, jaringan sudah terinfeksi dan pengguna tidak bisa berbuat banyak." kata Ken Low, praktisi keamanan berkualifikasi *Certified Information Security Proffessional (CISSP).*

*Active IDS* merupakan teknologi cikal bakal IPS yang mampu secara aktif mendeteksi serangan dan mengubah aturan firewall dan router untuk mengantisipasi serangan, dinilai mengganggu, sehingga tidak diterima oleh para administrator jaringan. Pada perkembangannya, frekuensi serangan terhadap jaringan meningkat sementara rentang waktu antara ditemukannya celah keamanan dan tersedianya patch untuk mentup celah itu, semakin sempit. Akibatnya, para administrator jaringan tidak memiliki cukup waktu untuk mengantisipasi serangan dengan memasang patch. Kondisi di mana serangan muncul sebelum tersedia patch disebut juga *Zero Day Attack*. Kemudian perkembangan teknologi memungkinkan IPS bekerja lebih cepat dalam menganalisa pola-pola serangan.

Salah satu merek peranti IPS bahkan memiliki kecepatan maksimal hingga lima Gigabit per detik (Gbps). IPS pertama kali diperkenalkan One Secure yang kemudian dibeli NetScreen Technologies sebelum akhirnya diakuisisi Juni per Neetworks pada 2004. Salah satu produsen IPS – Tip-ping-Point – juga dibeli penyedia peranti jaringan 3Com Corp. Sistem setup pada IPS sama dengan sistem setup pada IDS. IPS bisa sebagai host-based IPS (HIPS) yang bekerja untuk melindungi aplikasi dan juga sebagai network based IPS (NIPS). Mengapa

IPS lebih unggul dari IDS? Karena IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Tidak seperti IDS, secara logika IPS akan menghalangi suatu serangan sebelum terjadi eksekusi pada memori.

### 3.7. SQL Injection

Injeksi *SQL* adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan *SQL* atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Pada dasarnya sql injection adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain.

### *3.8. Denial Of Service (DOS)*

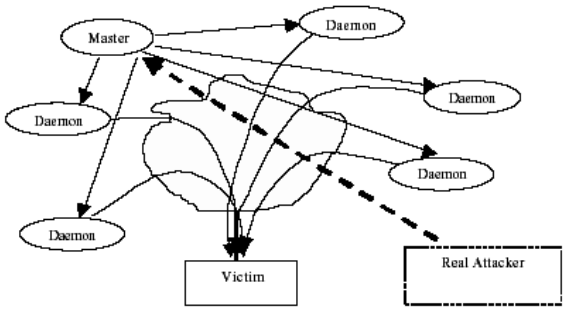
Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu).

Pada dasarnya Denial of Service merupakan serangan yang sulit diatasi, hal ini disebabkan oleh resiko layanan publik dimana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang kita tahu, keyamanan berbanding terbalik dengan keamanan. Maka resiko yang mungkin timbul selalu mengikuti hukum ini.

Wood (2003) DoS attack ditandai oleh usaha attacker untuk mencegah legitimate user dari penggunaan resource yang diinginkan. Adapun beberapa metode untuk melakukan DoS attack sebagai berikut:

i. Mencoba untuk membanjiri (flood) network, dengan demikian mencegah lalu lintas yang legitimate pada network.
ii. Mencoba mengganggu koneksi antara dua mesin, dengan demikian mencegah suatu akses layanan.
iii. Mencoba untuk mencegah individu tertentu dari mengakses layanan.
iv. Mencoba untuk mengganggu layanan sistem yang spesifik atau layanan itu sendiri.

Format terdistribusi membuat dimensi menjadi "*many to one*", dimana jenis serangan ini lebih sulit untuk dicegah. DDoS adalah terdiri dari 4 elemen seperti gambar 2.6 dibawah ini .




***Gambar 4. Empat elemen DDoS attack.***

Empat elemen tersebut adalah:

1. Korban (victim) yakni host yang dipilih untuk diserang.
2. Attack Daemon Agents, merupakan program agen yang benar-benar melakukan serangan pada target korban. Serangan daemon biasanya menyebar ke computer-komputer host. Daemon ini mempengaruhi target dan komputer-komputer host. Manfaat serangan daemon ini dipergunakan attacker untuk untuk memperoleh akses dan menyusup ke komputer-komputer host.
3. Kendali Program Master, Yakni Tugasnya adalah untuk mengkoordinir serangan.
4. Attacker (penyerang), yakni penyerang riil, dalang di belakang serangan.

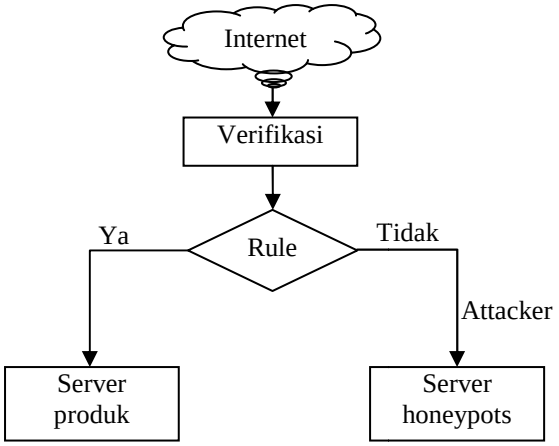
Dengan penggunaan kendali master program, penyerang riil dapat berdiri dibelakang layer dari serangan. Langkah-Langkah yang berikut berlangsung pada saat serangan terdistribusi:

i. Penyerang riil mengirimkan suatu "execute" pesan kepada kendali master program.
ii. Kendali master program menerima "execute" pesan kemudian menyebarkan perintah ini kepada attack daemons dibawah kendalinya.
iii. Ketika menerima perintah penyerangan, attack daemons mulai menyerang korban (victim).

Walaupun nampaknya penyerang riil hanya melakukan sedikit pekerjaan disini, namun dengan melakukan pengiriman "execute" command, dia sebenarnya telah merencanakan pelaksanaan DDoS attacks. Attacker harus menyusup ke semua komputer host dan network dimana daemon attacker dapat disebar. Attacker harus mempelajari topologi jaringan target, kemudian melakukan pencarian bottlenecks dan kelemahan jaringan untuk dimanfaatkan selama serangan. Oleh karena penggunaan attack daemon dan kendali master program, penyerang real tidak secara langsung dilibatkan sepanjang searangan, dimana keadaan ini membuat dia sulit dilacak sebagai pembuat serangan.

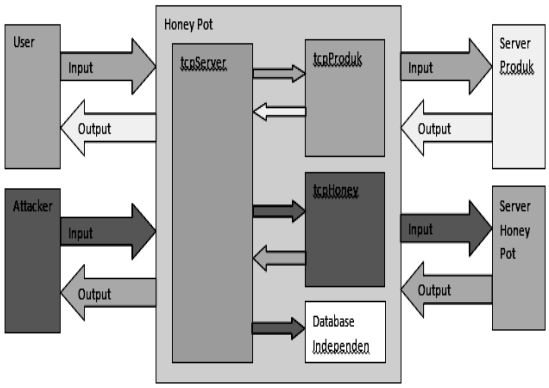
## *4. METODOLOGI PENELITIAN*

Secara umum kerangka pemikiran sistem honeypots yang akan dirancang digambarkan seperti terlihat pada gambar 3.1 sebagai berikut:




***Gambar 5. Konsep kerja system Honeypots***

Logika dari system honeypots tersebut dapat dilihat pada gambar 3..2 sebagai berikut.

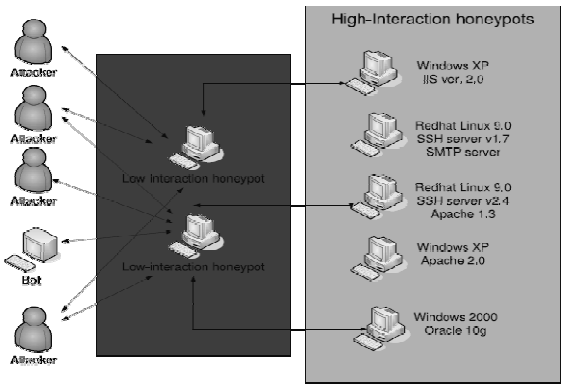



***Gambar 6. Logika system Honeypots***

Dari gambar diatas dapat dijelaskan bahwa input dari User maupun Attacker akan di respon oleh tcpServer yang akan memilah input. Jika input tersebut mengandung kata-kata atau kalimat yang sama dengan aturan yang telah tersimpan di database independen, maka tcpServer akan mengirimkan data ke tcpHoney yang akan melanjutkan input menuju ke server honeypots, serta menerima output dari server honeypots dan mengirimkan kembali ke tcpServer, dan tcpServer akan melanjutkan output ke attacker.

Tetapi jika input **tidak** mengandung kata-kata atau kalimat yang sama dengan aturan yang telah tersimpan di database independen, maka tcpServer akan mengirimkan data ke tcpProduk yang akan melanjutkan input menuju ke server produk, serta menerima output dari server produk dan mengirimkan kembali ke tcpServer, dan tcpServer akan melanjutkan output ke user.

Keseluruhan blok diagram sistem dapat dilihat pada diagram alur kerja sistem honeypot pada gambar 3.3.




***Gambar 7. Diagram alur kerja sistem honeypots***

### *4.1. Instalasi*

Pada penelitian ini akan digunakan 3 unit komputer dengan sistem operasi windows Xp service pack 2, dimana diantaranya adalah sebagai server produk, server honeypot dan komputer attacker.

Kemudian setelah jaringan fisik terpasang maka dapat dilakukan setting IP kelas C satu area sehingga 3 unit komputer tersebut dapat terhubungan dengan baik.

Kabutuhan software pendukung pada penelitian ini adalah visual basic 6.0, kemudian untuk mempermudah konfigurasi program visual Basic terhadap jaringan dapat ditambahkan software pendukung yaitu tcp server dan componen One.

### *4.2. Konfigurasi Honeypot*

Setelah kebutuhan perangkat keras dan perangkat lunak terpenuhi kemudian dapat dilakukan konfigurasi sistem honeypot, dalam hal ini adalah menentukan komputer yang akan dipergunakan sebagai server produk, server honeypot dan komputer attacker.

Konfigurasi honeypot dapat dilakukan pada posisi running yaitu dengan melakukan setting IP dan port yang akan dipergunakan dalam proses pengujian.

### *4.3. Pengujian honeypot*

Proses pengujian sistem honeypot akan dilakukan dua tahap pengujian, dimana tahap pertama adalah server produk diserang dengan komputer attacker pada kondisi tanpa sistem honeypot. Tahap kedua adalah server produk diserang oleh komputer attacker dimana sistem honeypot yang telah dirancang dalam posisi running atau aktif.

### *4.4. Evaluasi*

Perancangan dan implementasi sistem honeypot ini ditulis berdasarkan teori dan dari berbagai macam sumber. Jika pada implemntasi terdapat perubahan baik disegi hardware maupun software maka akan dilakukan pembenahan.

### *4.5. Implementasi*

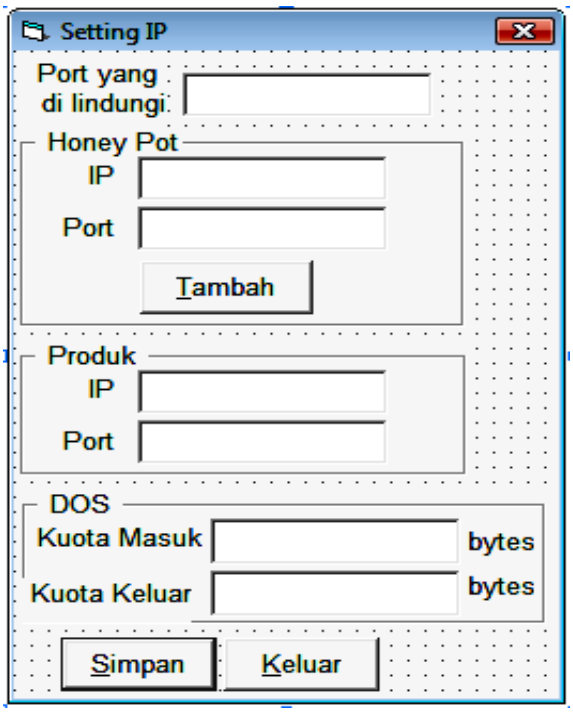
Implementasi untuk penelitian ini dilakukan dengan menggunakan fasilitas laoratorium jaringan komputer Universitas Muhammadiyah Sidoarjo, dengan sarana peralatan yang cukup untuk mengimplementasikan sistem honeypot yang telah penulis rancang.

## *5. IMPLEMENTASI DAN PENGUJIAN*

### 5.1. Perancangan sistem

#### i. Setting IP

Menu Ip digunakan untuk menyimpan IP dan port yang akan di gunakan dalam program honey pot.




*Gambar 8. Form setting*

Form Setting IP merupakan fom utama system honeypot dalam pengalamatan terhadap sebuah workstation. Gambar diatas menunjukkan bahwa port yang digunakan honeyport sama dengan port yang dugunakan oleh Appserv, sehingga untuk menggunakannya port Appserv dapat diganti dengan port yang belum digunakan oleh aplikasi lain. Sedangkan pada pengaturan honeypots terdapat menu Tambah, menu tersebut digunakan jika administrator menggunakan lebih dari satu server honeypots dengan ketentuan rule sql injection akan diarahkan pada server honeypots pertama dan rule DoS diarahkan pada server honeypots kedua. Adapun keterangan fungsi dari form tersebut dapat dilihat pada tabel 4.1.

*Tabel 3. Tabel keterangan form setting*

| Menu | Fungsi |
|---|---|
| Port yang di lindungi | Di isi dengan port yang akan di lindungi oleh program honey pot. Contoh : port 80 (port World Wide Web) |
| IP Honey Pot | Di isi dengan alamat IP dari database yang akan menjadi honey pot |
| Port Honey Pot | Di isi dengan port dari database yang akan menjadi honey pot. Port ini dipisahkan dari port yang akan di lindungi karena WinSock tidak bisa memantau port yang sudah di pantau oleh program lain (bentrok). Error lihat di gambar di bawah |
| IP Produk | Di isi dengan alamat IP dari database produk |
| Port Produk | Di isi dengan port dari database produk |

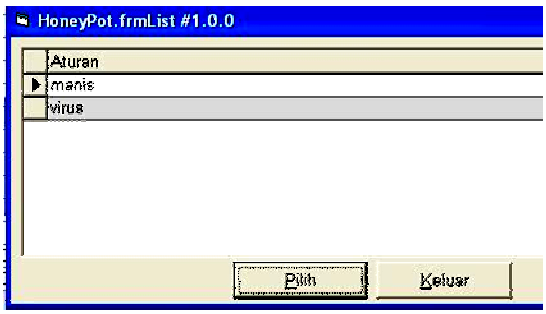
#### ii. Setting Aturan

Form setting aturan adalah sebuah menu yang berfungsi untuk mengatur berbagai aturan-aturan atau rule sql injection yang di pakai di program honey pot. Form setting aturan dapat dilihat pada gambar 4.2 sebagai berikut :


*Gambar 9. Form setting aturan (rules honeypots)*

Button Lihat merupakan button yang berfungsi untukk menampilkan berbagai aturan yang telah ditentukan oleh administrator sistem informasi.

Contoh tampilan aturan dapat dilihat pada gambar berikut :




*Gambar 10. daftar form rules*

Kehandalan fungsi dari form aturan setting tersebut sangat ditentukan oleh administrator maka untuk meningkatkan nilai guna dari aturan tersebut dapat dilakukan dengan updateting rule sql injection secara kontinu. Demikian pula sebaliknya jika administrator memasukkan aturan aturan yang salah maka hal tersebut dapat membahayakan keamanan dari sistem informasi.

Adapun detil rincian dari menu setting aturan dapat lihat pada gambar 4.2 sebagai berikut :

***Tabel 4. Tabel keterangan form setting aturan***

| **Nama Tombol** | **Keterangan** |
|---|---|
| Lihat | Jika tombol Lihat di tekan akan muncul form list yang menampilkan aturan-aturan yang ada di dalam program honey pot.<br>Di form list ada 2 tombol :<br>**Pilih** : Di gunakan untuk memilih aturan yang ada di dalam program honey pot. Sehingga aturan tersebut bisa di ubah atau dihapus.<br>**Keluar** : Di gunakan untuk keluar dari form list kembali ke form Setting Aturan |
| Hapus | Di gunakan untuk menghapus aturan. |
| Keluar | Di gunakan untuk kembali ke program utama. |

### iii. Bersihkan Log

Menu bersihkan log di gunakan untuk membersihkan data log. Sehingga untuk mengosongkan aturan yang telah tersimpan dalam database dapat dilakukan dengan menekan button tersebut.

## 5.2. Implementasi dan konfigurasi sistem

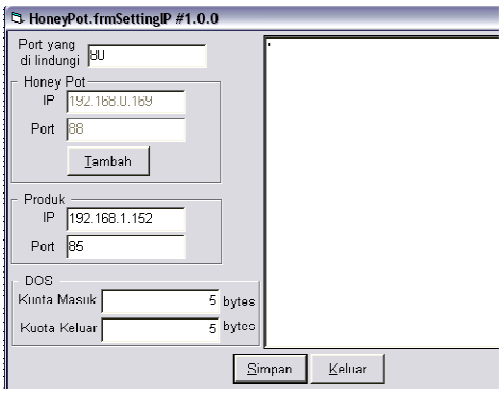
Dalam form utama ini pengguna dapat melihat seluruh fungsi yang ada pada system honeypot. Dalam form ini terdapat terdapat report IP, Tanggal dan Keterangan. Keterangan IP dalam form ini menunjukkan bahwa system telah mendeteksi adanya serangan dari alamat IP yang terlapor. Report tanggal merupakan laporan waktu terjadinya serangan dan report keterangan merupakan detil jenis serangan yang telah dilancarkan oleh attacker.


***Gambar 11. Form Utama***

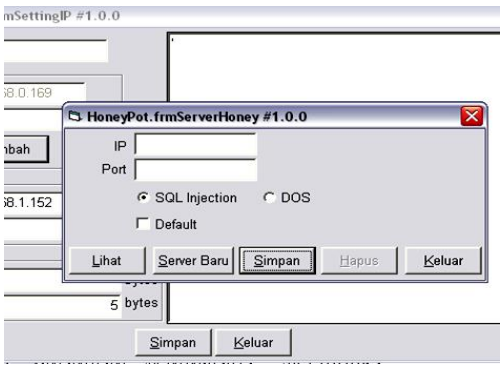
### i. Setting IP

Form setting IP terdapat pada menu dropdown yang terdapat pada menu pengaturan pada form utama. Pada pengujian ini penulis manginputkan port yang dilindungi dengan port 80 sebagai default, karena secara umum port yang di request oleh user adalah port Http. Honey Pot diinputkan dengan Ip dan Port webserver komputer yang akan dijadikan sebagai server umpan. Produk diinputkan dengan IP dan Port webserver yang dilindungi dari serangan attacker.

Sedangkan Kuota diinputkan dengan batasan request yang diinginkan oleh administrator karena masing-masing webserver memiliki batasan kuota yang berbeda pula. Setelah setting port ini telah lengkap maka administrator dapat menyimpan dengan menekan button simpan dan kemudian keluar untuk melakukan setting rule.




***Gambar 12. Form setting IP***

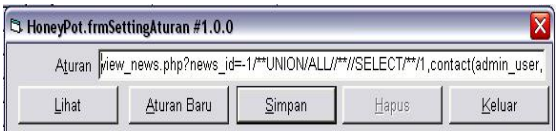



***Gambar 13. Tampilan menu Tambah IP***

**ii. Setting Aturan**

Form ini diperuntukkan untuk mendeteksi serangan Sql Injection, cara kerjanya adalah dengan menginputkan berbagai contoh perintah sql injection, semakin banyak aturan yang dimasukkan maka semakin komplek pula rule pada program honeypot.

Contoh perintah sql injection yang diinputkan akan disimpan dalam database yang kemudian akan dijadikan sampel jika honeypot mendapat http request maka program akan memeriksa apakah request tersebut apakah request tersebut memiliki kesamaan pola dengan contoh perintah sql injection yang telah diinputkan, jika memiliki kesamaan pola maka program akan membelokkan request tersebut ke server honeypot yang telah ditentukan alamat Ip dan portnya. Jika tidak memiliki kesamaan maka request tersebut diteruskan ke server produk.




***Gambar 14. Form Setiing aturan***

Untuk mengetahui rule yang telah ada dalam database dapat dilakukan dengan menekan tombol lihat, sehingga terlihat seperti pada gambar dibawah ini.


***Gambar 15. Detil form setting aturan***

**5.3. Pengujian sistem**

**i. *Pengujian Sql Injection***

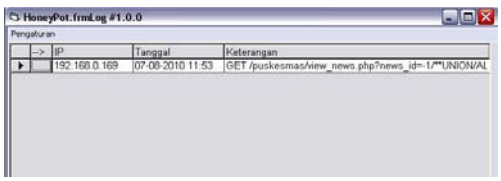
Untuk melakukan pengujian Sql injection dibutuhkan sebuah browser untuk melakukan request sql injection dengan server sasaran yang telah ditentukan, dalam pengujian ini penulis menggunakan Mozila firefox 4.6. Untuk melakukan sql injection pertama yang harus dilakukan adalah melakukan cek adanya kesalahan, kemudian yang dapat dilakukan adalah mencari dan menghitung jumlah table yang ada dalam databasenya


***Gambar 16. Contoh perintah sql injection order by***

Adapun contoh sql injection menggunakan Union seperti gambar 4.10 berikut :

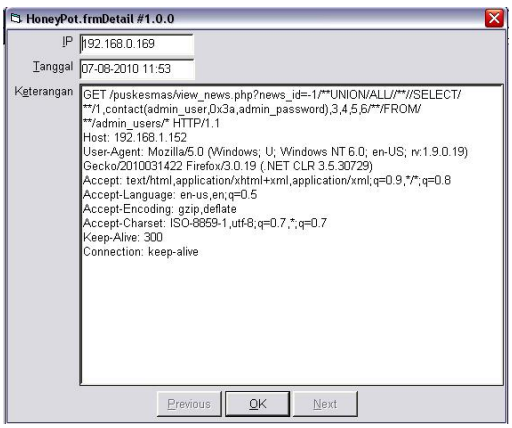
***Gambar 17. Contoh perintah sql injection UNION***

Kemudian pada sisi program honeypot dapat kita lihat terdapat sebuah report, dimana report tersebut mengindikasikan adanya serangan yang dilakukan oleh seorang attacker seperti terlihat pada gambar 4.13




***Gambar 18. Report indikasi adanya serangan attacker***

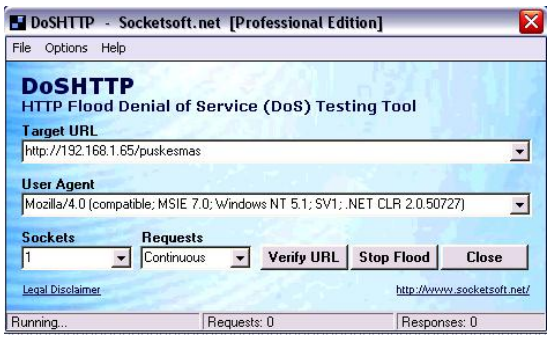
Pada gambar di atas bahwa request tersebut bukan merupakan request normal, karena halaman tersebut tidak terdapat pada webserver. Dengan demikian dapat disimpulan bahwa program honeypot telah berhasil mendeteksi adanya serangan Sql Injection




***Gambar 19. Detil report serangan sql injection***

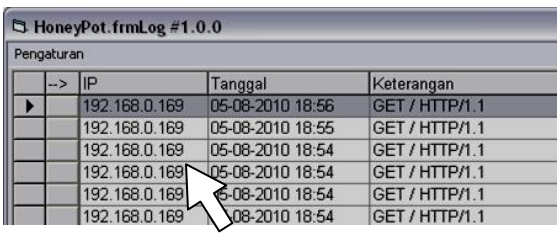
**ii. *Pengujian Denial of Service (DoS)***

Untuk melakukan pengujuan Denial of Service dibutuhkan sebuah tool yang dapat kita download secara gratis di internet. Dalam pengujian Denial of Service ini penulis menggunakan tool DosHttp 2.0. Perlu diketahui karena program ini hanya mengemulasikan service Denial of Service maka ketentuannya adalah satu IP dengan satu socket, terlihat pada gambar 4.13 dibawah ini.



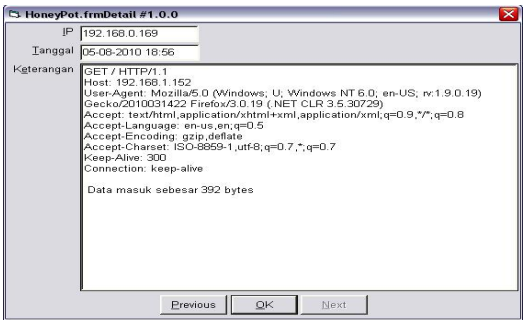

***Gambar 20. DosHttp 2.0***

Untuk melakukan uji terhadap sistem honeypot yang telah dirancang dapat dilakukan dengan menkan tombol Start floading seperti gambar diatas. Kemudian pada sisi sistem honeypot akan tampil indikasi adanya serangan tersebut, sehingga dapat dilihat seperti pada gambar 4.14 berikut.




***Gambar 21. Report indikasi adanya serangan attacker***

Gambar di atas membuktikan bahwa program telah menerima indikasi adanya serangan dari attacker yang terlihat pada form utama, kemudian untuk mengetahui detils serangan dapat dilakukan




***Gambar 22. Detil report serangan denial of service***

Berikut adalah form detil yang menunjukkan serangan yang dilakukan oleh attacker secara rinci, dalam gambar dibawah terlihat bahwa data masuk sebesar 392 bytes yang ini menandakan bahwa request yang dilakukan oleh user dengan IP 192.168.0.169 bukan merupakan request biasa karena melebihi ukuran kuota yang telah ditentukan yaitu sebesar 50 byte. Sehingga dapat disimpulkan client tersebut telah melakukan serangan berupa Denial of Service dan program honeypot telah berhasil memberikan service terladap lay

## *6. SIMPULAN*

Sistem honeypot yang telah dirancang dalam penelitian ini telah berhasil mendeteksi indikasi adanya bahaya yang sedang mengancam web server yang berupa sql injection dan denial of service kemudian memberikan service terhadap request berupa sql injection dan denial of service dengan cara membelokkan request kedua jenis serangan tersebut ke server honeypot.

1. Berdasarkan dari analisa terhadap percobaan tersebut, terlihat bahwa honeypot memiliki kekurangan. Kekurangan terbesar berasal dari keterbatasan pandangan, karena system tersebut hanya menangkap aktivitas yang diarahkan pada system produk, dan tidak menangkap serangan pada system yang lain. Jika terdapat banyak server di server farm selain server tersebut yang diserang oleh attacker, maka serangan tersebut tidak dapat deteksi oleh honeypot.
2. Sistem honeypot telah berhasil meringankan tugas dari deteksi menjadi lebih sederhana, efektif dan murah. Konsepnya sendiri sangat mudah dipahami dan diimlementasikan. Honeypot sendiri ditujukan untuk mendeteksi serangan ayng dilakukan oleh attacker dengan mengecoh attacker tersebut dengan fasilitas mirror server.
3. Sistem honeypot yang digunakan penulis merupakan honeypots high interaction dengan rule sql injection dan danial of service (DoS), kedua rule tersebut bukanlah merupakan rule yang tergolong aman untuk sebuah system informasi yang besar, karena masih banyak type serangan yang bisa dilakukan oleh seorang attacker.

## *7. SARAN*

Berdasarkan dari analisa terhadap percobaan tersebut, terlihat bahwa honeypot memiliki berbagai kekurangan oleh karena itu peneliti memberikan beberapa saran sebagai berikut:

1. Honeypot dapat digunakan untuk menambah keamanan web server, namun tidak dapat menggantikan system keamanan yang lain diantaranya adalah firewall dan Intrusion detection system (IDS).selalu update rule honeypot, perbanyak rule honeypots dan penerapan teknologi neural network sangat mendukung kemajuan system honeypot
2. Keterbatasan dalam penelitian ini baik waktu maupun pengetahuaan penliti sehingga dapat dilanjutkan peneliti-peneliti yang lain

## *DAFTAR PUSTAKA*


1. **Computer Security Institute**. Computer Security Issues & Trends vol. III no. 1, 2002. Computer Security Institute.
2. **Honeynet Project**. Know Your Enemy : Honeynet, 2003. http://project.honeynet.org
3. **Honeynet Project**. Know Your Enemy : Defining Virtual Honeynets, 2003. http://project.honeynet.org
4. **Indrajit, Richardus Eko; Prastowo, B.N.; dan Yuliardi Rofiq**. Memahami Security Linux, 2002. Elex Media Komputindo
5. **Pressman, Roger S**. Software Engineering : A Practitioner's Approach – fourth edition, 1997. Mc-Graw Hill International Edition.
6. **Purbo, Onno W.** dan **Wiharjito, Tony**. Keamanan Jaringan Internet, 2000. Elex Media Komputindo
7. **Rudianto, Dudy**. Perl untuk Pemula, 2003. Elex Media Komputindo
8. **Spitzner, Lance**. Honeypots : Simple Cost – Effective Detection, 2003. http://www.securityfocus.com
9. **Spitzner, Lance**. Honeypots : Definitions and Value of Honeypots, 2003. http://www.tracking-hackers.com
10. **Sulistyo, Eko, Tribroto Harsono, Fazmah Arif Yulianto**. Studi Implementasi Honeypot Sebagai Salah Satu Alat Deteksi Pada Keamanan Jaringan, 2003. STTTelkom
11. **Wood, D, Anthony, Stankovic, A, John**, "Denial of Service in Sensor Networks", http://www.cs.virginia.edu/~adw5p/pubs/computer02-dos.pdf, Oktober 2003